CSM - Hoe u SSL-certificaten van derden voor GUI-toegang installeert

Inhoud

Inleiding

Cisco Security Manager (CSM) biedt een optie om beveiligingscertificaten te gebruiken die zijn afgegeven door certificeringsinstanties van derden (CA's). Deze certificaten kunnen worden gebruikt wanneer het organisatiebeleid voorkomt dat CSM-zelf-ondertekende certificaten worden gebruikt of eist dat systemen een certificaat gebruiken dat is verkregen van een bepaalde CA.

TLS/SSL gebruikt deze certificaten voor communicatie tussen de CSM Server en de client browser. Dit document beschrijft de stappen om een certificaataanvraag (CSR) te genereren in CSM en hoe de identiteit en de basiscertificaten van CA in hetzelfde proces moeten worden geïnstalleerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van SSL-certificaten Architectuur.
- Basiskennis van Cisco Security Manager.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Security Manager versie 4.1.1 en hoger.

CSR-aanmaak vanuit gebruikersinterface

In dit hoofdstuk wordt beschreven hoe een CSR moet worden gegenereerd.

Stap 1. Start de startpagina van Cisco Security Manager en selecteer **Server Administration > Server > Security > Single-Server Management > certificaatinstelling.**

Stap 2. Voer de waarden in die vereist zijn voor de velden die in deze tabel zijn beschreven:

Veld	Gebruik opmerkingen
Naam van land	Landcode van twee tekens.
Staat of provincie	De naam van de staat of provincie of de volledige naam van de provincie.
Locatie	Twee personages of stadscode of de volledige naam van de stad of stad.
Naam van organisatie	Volledige naam van uw organisatie of afkorting.
Naam van organisatie	Volledige naam van uw afdeling of een afkorting.
Servernaam	DNS naam, IP adres of hostnaam van de computer. Voer de servernaam in met een juiste en oplosbare domeinnaam. Dit wordt weergegeven o uw certificaat (al dan niet door henzelf getekend of door derden afgegeven). Lokale gasthe of 127.0.0.1 dient niet te worden vermeld.
E-mailadres	E-mailadres waarop de post moet worden verstuurd.

Stap 3. Klik op **Toepassen** om de CSR te maken.

Het proces genereert de volgende bestanden:

- de privé-sleutel van de server.key—server.
- server.crt—het zelfgetekende certificaat van de server.
- Server.pk8—de privé sleutel van de server in PKCS#8 formaat.

- server.csr-CSR-bestand (certificaataanvraag) gebruikt.

Opmerking: dit is het pad voor de gegenereerde bestanden.
~CSCOpx\MDC\Apache\conf\ssl\chain.cer
~CSCOpx\MDC\Apache\conf\ssl\server.crt
~CSCOpx\MDC\Apache\conf\ssl\server.csr
~CSCOpx\MDC\Apache\conf\ssl\server.pk8
~CSCOpx\MDC\Apache\conf\ssl\server.key

Opmerking: Als het certificaat een automatisch ondertekend certificaat is, kunt u deze informatie niet wijzigen.

Uploaden van identiteitsbewijzen in CSM-server

In deze sectie wordt beschreven hoe het identiteitsbewijs dat door de CA is meegeleverd, naar de CSM server kan worden geüpload

Stap 1 Vind het SSL Utility Script beschikbaar op deze locatie

```
NMSROOT\MDC\Apache
```

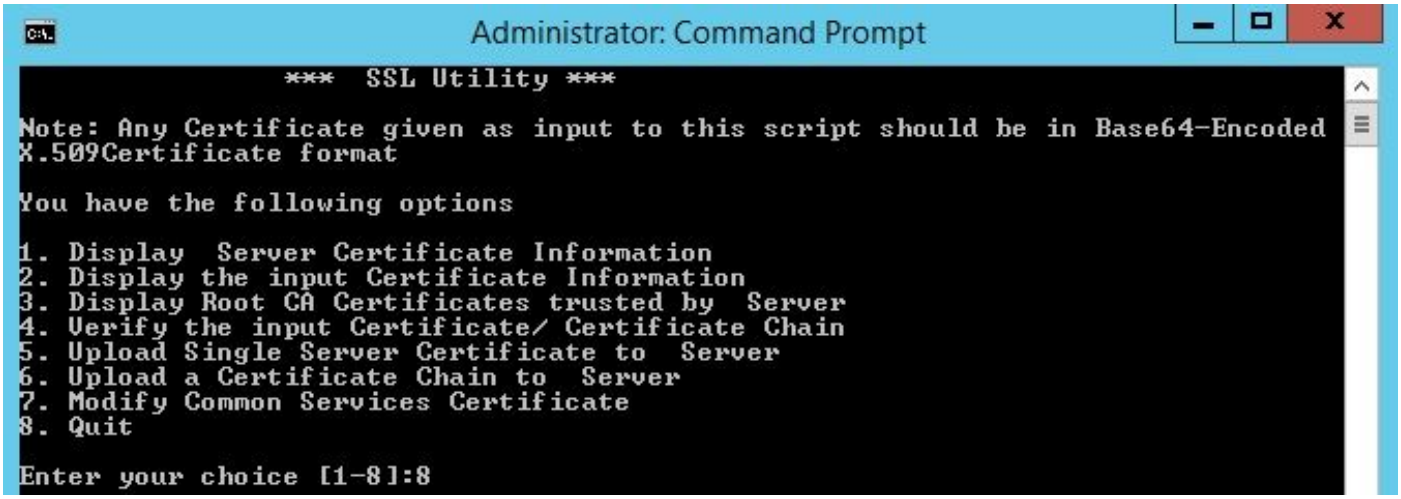
Opmerking: NMSROOT moet worden vervangen door de map waarin CSM is geïnstalleerd.

Deze voorziening heeft deze opties.

Nummer	Optie	Wat het doet...
1	Informatie over servercertificaat weergeven	• Hiermee geeft u de certificaatgegevens van de CSM-server weer. Voor certificaten van derden geeft deze optie de details weer van het servercertificaat, de (eventuele) tussencertificaten en het CA-certificaat (Opstarten).
2	Informatie over het invoercertificaat weergeven	• Controleer of het certificaat geldig is. Met deze optie accepteert u een certificaat als invoer en: • Controleer of het certificaat in gecodeerde X.509-certificaatindeling • Hiermee geeft u het onderwerp van het certificaat en de gegevens het uitgevende certificaat weer. • Controleer of het certificaat geldig is op de server.
3	Root CA-certificaten vertrouwen op de server	genereert een lijst met alle CA-certificaten die u hebt ontvangen.
4	Controleer het invoercertificaat of de certificeringsketen	Controleer of het servercertificaat dat is afgegeven door CA's van derd kan worden geüpload. Wanneer u deze optie kiest, gebruikt u: • Controleer of het certificaat in Base64 Encoded X.509certificaatfor is. • Controleer of het certificaat geldig is op de server • Verifieer of de privé sleutel van de server en de input server certifi match. • Verifieer of het servercertificaat kan worden gevolgd naar het verei

		CA-certificaat dat gebruikt is om het te traceren. • Constructeert de certificeringsketen, als ook de intermediaire keter worden gegeven, en verifieert of de keten eindigt met het juiste CA certificaat. Nadat de verificatie is voltooid, wordt u gevraagd de certificaten te uplo naar de CSM Server. De voorziening geeft een fout weer: • Als de invoercertificaten niet in de vereiste indeling zitten • Indien de certificaatdatum niet geldig is of indien het certificaat ree verstreken. • Als het servercertificaat niet kan worden geverifieerd of getraceerd een basiscertificaat van CA. • Indien een van de tussentijdse certificaten niet als input werd verst • Als de privétoets van de server ontbreekt of als het servercertificaa wordt geüpload niet kan worden geverifieerd met de privé-sleutel v server. U moet contact opnemen met de CA die de certificaten heeft afgegeve deze problemen te corrigeren voordat u de certificaten naar CSM uploa U moet de certificaten met optie 4 controleren voordat u deze optie selecteert. Selecteer deze optie, alleen als er geen intermediaire certificaten zijn e alleen het servercertificaat is ondertekend door een vooraanstaande R CA-certificaat. Als de hoofdlettertoets niet door CSM is vertrouwd, selecteert u deze o niet. In dergelijke gevallen dient u een CA-certificaat te verkrijgen dat gebrui wordt voor het ondertekenen van het certificaat via de CA-indeling en b certificaten te uploaden via optie 6. Wanneer u deze optie selecteert en de locatie van het certificaat opgee gebruikt u: • Controleer of het certificaat in Base64 Encoded X.509-indeling is. • Hiermee geeft u het onderwerp van het certificaat en de gegevens het uitgevende certificaat weer. • Controleer of het certificaat geldig is op de server. • Verifieert of de server private key en de input server certificatie ma • Verifieer of het servercertificaat kan worden gevolgd naar het verei Root CA certificaat dat voor het tekenen is gebruikt. Nadat de verificatie met succes is voltooid, uploadt de voorziening het certificaat naar CiscoWorks Server. De voorziening geeft een fout weer: • Als de invoercertificaten niet in de vereiste indeling zitten • Indien de certificaatdatum niet geldig is of indien het certificaat ree verstreken. • Als het servercertificaat niet kan worden geverifieerd of getraceerd een basiscertificaat van CA. • Als de privétoets van de server ontbreekt of als het servercertificaa wordt geüpload niet kan worden geverifieerd met de privé-sleutel v server. U moet contact opnemen met de CA die de certificaten heeft afgegeve deze problemen te corrigeren voordat u de certificaten in CSM opnieuw
5	Eén servercertificaat uploaden naar de server	

		uploadt. U moet de certificaten met optie 4 controleren voordat u deze optie selecteert. Selecteer deze optie als u een certificeringsketen uploadt. Als u ook he basiscertificaat van CA uploadt, moet u dit als een van de certificaten i keten toevoegen. Wanneer u deze optie selecteert en de locatie van de certificaten opge gebruikt u: • Controleer of het certificaat in Base64 Encoded X.509 certificaatfo is. • Hiermee geeft u het onderwerp van het certificaat en de gegevens het uitgevende certificaat weer. • Controleer of het certificaat geldig is op de server • Controleer of server private key en de server certificatie match zijn • Verifieer of het servercertificaat kan worden gevolgd naar het basiscertificaat van CA dat voor het tekenen is gebruikt. • Constructeert de certificeringsketen, als er intermediaire ketens wo gegeven en verifieert of de keten eindigt met het juiste basiscertific CA.
6	Een certificeringsketen naar server uploaden	Nadat de verificatie met succes is voltooid, wordt het servercertificaat geüpload naar CiscoWorks Server. Alle intermediaire certificaten en het certificaat van de Opstarten worde geüpload en gekopieerd naar de CSM TrustStore. De voorziening geeft een fout weer: • Als de invoercertificaten niet in de vereiste indeling zijn. • Indien de certificaatdatum niet geldig is of indien het certificaat ree verstreken. • Als het servercertificaat niet kan worden geverifieerd of getraceerd een basiscertificaat van CA. • Indien een van de tussentijdse certificaten niet als input werd verm • Als de privétoets van de server ontbreekt of als het servercertificaa wordt geüpload niet kan worden geverifieerd met de privé-sleutel v server. U moet contact opnemen met CA die de certificaten heeft afgegeven o deze problemen te corrigeren voordat u de certificaten in CiscoWorks opnieuw uploadt.
7	Gemeenschappelijk servicescertificaat wijzigen	Met deze optie kunt u de ingang van de Host Name in het Gemeenschappelijk Servicecertificaat wijzigen. U kunt een alternatieve naam opgeven als u het bestaande item Host N wilt wijzigen.



Stap 2 Gebruik **optie 1** om een kopie van het huidige certificaat te verkrijgen en op te slaan voor raadpleging in de toekomst.

Stap 3 Stop de CSM Daemon Manager met deze opdracht in Windows Opdrachten voordat u het certificaatuploadproces start.

```
net stop crmdmgtd
```

> **Opmerking**: CSM services worden gedempt met deze opdracht. Zorg ervoor dat er tijdens deze procedure geen implementaties actief zijn.

Stap 4 Open SSL-hulpprogramma één keer. Dit hulpprogramma kan geopend worden met behulp van de Opdrachtmelding door naar het eerder genoemde pad te navigeren en deze opdracht te gebruiken.

```
perl SSLUtil.pl
```

Stap 5 Selecteer **optie 4**. **Controleer de invoer van het certificaat/de certificaatketen.**

Stap 6 Voer de locatie van de certificaten in (servercertificaat en intermediair certificaat).

> **Opmerking**: Het script verifieert of het servercertificaat geldig is. Nadat de verificatie is voltooid, geeft de voorziening de opties weer. Als het script fouten meldt tijdens validatie en verificatie, geeft het SSL Utility instructies om deze fouten te corrigeren. Volg de instructies om deze problemen op te lossen en probeer dezelfde optie één keer.

Stap 7 Selecteer een van de volgende twee opties.

Selecteer **Optie 5** als er slechts één certificaat is om te uploaden, dat wil zeggen als het servercertificaat is getekend door een CA-certificaat (Opstarten).

> **OF**

Selecteer **Optie 6** als er een certificaatketen is om te uploaden, dat wil zeggen als er een servercertificaat en een tussentijds certificaat is.

Opmerking: CiscoWorks staat niet toe om te uploaden als CSM Daemon Manager niet is gestopt. De voorziening geeft een waarschuwingsbericht weer als er hostname-miswedstrijden zijn gedetecteerd in het servercertificaat dat wordt geüpload, maar het uploaden kan worden voortgezet.

Stap 8 Voer deze vereiste gegevens in.

- Plaats van het certificaat
- Eventuele locatie van tussentijdse certificaten.

SSL Het hulpprogramma uploadt de certificaten als alle details correct zijn en de certificaten aan CSM vereisten voor veiligheidscertificaten voldoen.

Stap 9 Start de CSM Daemon Manager opnieuw om de nieuwe wijziging te laten uitvoeren en CSM-services mogelijk te maken.

```
net start crmdmgtd
```

Opmerking: wacht op een totaalbedrag van 10 minuten om alle CSM-services opnieuw te starten.

Stap 10 Bevestig dat de CSM het geïnstalleerde identiteitsbewijs gebruikt.

Opmerking: Vergeet niet om de root- en intermediaire CA-certificaten in de PC of server te installeren vanaf waar de SSL-verbinding is gestabiliseerd op de CSM.